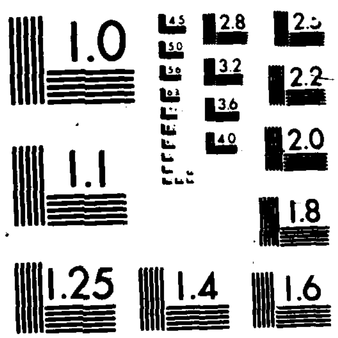
AD-A172 771 ON THE THEORY AND PRACTICE OF MULTI-DIM INDICES MOD M A CIRCULAR SLIDE-RU..(U) WISCONSIN UNIV-MADISON MATHEMATICS RESEARCH CENTER I J SCHOENBERG AUG 86 1/1

UNCLASSIFIED MRC-TSR-2955 DAAG29-80-C-0041 F/G 12/1 NL


1.0
2.8
3.2
2.2
3.6
4.0
2.0
1.1
1.8
1.25
1.4
1.6

MRC Technical Summary Report #2955

ON THE THEORY AND PRACTICE OF MULTI-DIM. INDICES mod m. A CIRCULAR SLIDE-RULE FOR THE MODULUS m = 100

I. J. Schoenberg

Mathematics Research Center
University of Wisconsin—Madison
610 Walnut Street
Madison, Wisconsin 53705

August 1986

(Received August 21, 1986)

Sponsored by

U. S. Army Research Office
P. O. Box 12211
Research Triangle Park
North Carolina 27709

UNIVERSITY OF WISCONSIN-MADISON
MATHEMATICS RESEARCH CENTER

ON THE THEORY AND PRACTICE OF MULTI-DIM. INDICES mod m. A CIRCULAR SLIDE-RULE FOR THE MODULUS $m = 100$

I. J. Schoenberg

Technical Summary Report #2955
August 1986

ABSTRACT

The paper establishes the following theorem of elementary Number Theory: Let

(1) $$m = m_1 m_2, \quad (m_1, m_2) = 1$$

and let

(2) a_i be a primitive root mod m_i $(i = 1,2)$.

We also assume that

(3) the modulus $m = m_1 m_2$ admits no primitive root.

By the Chinese Remainder Theorem applied twice we determine the solutions b_1 and b_2 of the two pairs of congruences

$$b_1 \equiv a_1 \bmod m_1, \quad b_2 \equiv 1 \bmod m_1,$$
$$b_1 \equiv 1 \bmod m_2, \quad b_2 \equiv a_2 \bmod m_2.$$

Then every element N of a reduced residue system mod m is furnished just once by the congruences

(4) $$N \equiv b_1^{x_1} b_2^{x_2} \bmod m \quad (N \geq 1,\ N \leq m-1),$$

where

(5) $$x_1 = 0,1,\ldots,\varphi(m_1) - 1, \quad x_2 = 0,1,\ldots,\varphi(m_2) - 1,$$

where $\varphi(m)$ is the Euler function.

We define the index of N mod m as the 2-dim. vector

(6) $$\operatorname{ind} N = (x_1, x_2).$$

Since b_i is a primitive root mod m_i $(i = 1,2)$ we can modify x_i mod $\varphi(m_i)$ $(i = 1,2)$.

The $1 - 1$ mapping $\{N\} \leftrightarrow \{(x_1,x_2)\}$, established by (4), between the <u>multiplicative</u> group $\{N\}$ mod m and the <u>additive</u> group $\{(x_1,x_2)\}$ (mod $\varphi(m_1)$, mod $\varphi(m_2)$) is an isomorphism.

Using this theorem the paper concludes with the construction of a circular slide-rule for the modulus $m = 100$, which admits no primitive root.

AMS (MOS) Subject Classifications: 10A10, 10A99

Key Words: Indices mod m as vectors, A circular slide-rule mod 100

Work Unit Number 6 (Miscellaneous Topics)

Sponsored by the United States Army under Contract No. DAAG29-80-C-0041.

SIGNIFICANCE AND EXPLANATION

~~The~~ paper defines indices for a modulus m which admits no primitive root, like the modulus $m = 100$. If $m = m_1 m_2$, with $(m_1, m_2) = 1$, and if m_1 has the primitive root a_1, and m_2 has the primitive root a_2, then the index of a number N, with $(N, m) = 1$, is defined by an appropriate 2-dimensional vector.

As an example we choose $m = 100$, $m_1 = 4$, $m_2 = 25$. The paper concludes with the construction of a circular slide-rule for the modulus $m = 100$.

The responsibility for the wording and views expressed in this descriptive summary lies with MRC, and not with the author of this report.

ON THE THEORY AND PRACTICE OF MULTI-DIM. INDICES mod m.

A CIRCULAR SLIDE-RULE FOR THE MODULUS $m = 100$

I. J. Schoenberg

1. **INTRODUCTION.** I wrote recently the note [2] on the Chinese Remainder Theorem (abbreviated to C.R.T.) which seems suitable as an elementary introduction to this important topic. The present note was written in connection with a one-semester course on elementary Number Theory given in 1975 at the San Diego State University. It was submitted then to the Classroom Notes section of the A. M. Monthly through its new editor R. A. Brualdi, but somehow it was forgotten. I found it now and wish to publish it as an attractive sequel to my first note [2]. Possibly its main innovation in 1975 was the introduction of the notion of indices mod m for numbers m which have no primitive roots in the classical sense, like $m = 100$: The indices introduced are multiply-dimensional vectors.

This was in 1975. At the present time we have the pioneering paper [1] by Ulrich Oberst who shows that by appropriate abstract formulations, the Chinese Remainder Theorem can be made the basis of much of Modern Algebra including the main theorems of *Galois* theory.

The present note assumes the reader to be familiar with the beautiful theory of primitive roots and indices for a modulus m which admits a primitive root. For these fundamental notions we refer to any book on Number Theory, for instance to Steward's book [3].

Sponsored by the United States Army under Contract No. DAAG29-80-C-0041.

2. **The Main Problem.** Let $\varphi(m)$ denote as usual Euler's function. The integer a is a primitive root mod m, provided that the $\varphi(m)$ powers

(1) $$N = a^I \quad (I = 0,1,\ldots,\varphi(m) - 1)$$

form a reduced residue system (R.R.S.) mod m. We also write

(2) $$I = \text{ind } N$$

and call it the <u>index</u> of N mod m. Notice that the sequence (1) can not be further extended, because $a^{\varphi(m)} \equiv 1$ mod m, by Euler's theorem.

We are here concerned with the following

Problem 1. Let

(3) $$m = m_1m_2, \quad (m_1,m_2) = 1, \quad m_1 > 1, \quad m_2 > 1 \ ,$$

and let

(4) $$a_i \text{ be a primitive root mod } m_i \quad (i = 1,2) \ .$$

We also assume that the product

(5) $$m = m_1m_2 \text{ has no primitive root } .$$

(6) Question: Is there a way of defining indices for the product m ?

The answer: Yes, there is a way, but <u>the indices</u> mod m <u>will be 2-dimensional vectors</u>

(7) $$I = (x_1,x_2), \ (x_1 = 0,1,\ldots,\varphi(m_1) - 1; \ x_2 = 0,1,\ldots,\varphi(m_2) - 1 \ .$$

3. **The modulus** $m = 100$. We are particularly interested in this modulus and choose

(8) $$m_1 = 4,\quad m_2 = 25,\quad m = 100\ .$$

To check the assumption (4) we notice that

(9) $$a_1 = 3 \text{ is a primitive root } \bmod 4\ .$$

Since $\varphi(4) = 2$, it follows that

(10) $$\text{the sequence } 3^I\ (I = 0,1) \text{ is a R.R.S. } \bmod 4\ .$$

Likewise

(11) $$a_2 = 2 \text{ is a primitive root } \bmod 25\ .$$

Since $\varphi(25) = 25 \cdot (1 - \frac{1}{5}) = 20$, the statement (11) is verified by the following table

(12)

I = ind N	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
N	1	2	4	8	16	7	14	3	6	12	24	23	21	17	9	18	11	22	19	13

Verifying for (8) our assumption (5) is a little more troublesome. This requires

Lemma 1. <u>For every integer</u> a <u>with</u>

(13) $$(a, 100) = 1$$

<u>we have</u>

(14) $$a^{20} \equiv 1 \bmod 100\ .$$

Notice that

(15) $$\varphi(100) = \varphi(4)\varphi(25) = 2\cdot 20 = 40\ .$$

Since (13) implies (14), we see that there is no element of a R.R.S. mod 100 which belongs to the exponent $40 = \varphi(100)$: The modulus $m = 100$ satisfies the assumption (5).

<u>Proof of Lemma 1.</u> From $\varphi(50) = \varphi(2)\varphi(25) = 20$, by Euler's theorem we have $a^{\varphi(50)} \equiv 1 \bmod 50$ or

(16) $$a^{20} \equiv 1 \bmod 50\ .$$

From (13) we see that a must be an odd number, $a = 2n + 1$ say, and so by the binomial theorem

$$a^{20} - 1 = (2n+1)^{20} - 1 = (2n)^{20} + \binom{20}{1}(2n)^{19} + \cdots + \binom{20}{19}(2n) .$$

Since all terms of this sum are divisible by 4 we find that

$$4 \mid a^{20} - 1 . \tag{17}$$

From (16) we obtain $a^{20} - 1 = 50k$ and now (17) shows that the factor k must be even, hence $k = 2m$ say, which implies the desired congruence (14).

Our answer to the question (6) is given by the following

Theorem 1. Let

$$m = m_1 m_2, \quad (m_1, m_2) = 1 , \tag{18}$$

and let

$$a_i \text{ be a primitive root } \bmod m_i \quad (i = 1,2) . \tag{19}$$

By the Chinese remainder theorem applied twice we determinie the solutions b_1 and b_2 of the two pairs of congruences

$$\begin{aligned} b_1 &\equiv a_1 \bmod m_1, & b_2 &\equiv 1 \bmod m_1 , \\ b_1 &\equiv 1 \bmod m_2, & b_2 &\equiv a_2 \bmod m_2 . \end{aligned} \tag{20}$$

Then every element N of a reduced residue system $\bmod m$ is furnished just once by the congruences

$$N \equiv b_1^{x_1} b_2^{x_2} \bmod m \quad (N \geq 1, N \leq m - 1) , \tag{21}$$

where

$$x_1 = 0,1,\ldots,\varphi(m_1) - 1, \quad x_2 = 0,1,\ldots,\varphi(m_2) - 1 . \tag{22}$$

Proof. The formula (21) and (22) gives the right number $\varphi(m_1)\varphi(m_2) = \varphi(m)$ of elements of a R.R.S. mod m. There remains to show that no two elements

$$N \equiv b_1^{x_1} b_2^{x_2}, \quad N' \equiv b_1^{x_1'} b_2^{x_2'} \tag{23}$$

are congruent mod m unless $x_1 = x_1'$ and $x_2 = x_2'$. We do this by contradiction. We assume

$$(x_1, x_2) \neq (x_1', x_2') , \tag{24}$$

and more specifically, we assume

$$x_2 \neq x_2' \tag{25}$$

and we are to prove that

$$N \not\equiv N' \bmod m \ . \tag{26}$$

Indeed the congruence

$$b_1^{x_1} b_2^{x_2} \equiv b_1^{x_1'} b_2^{x_2'} \bmod m \tag{27}$$

is impossible: Clearly (27) implies that

$$b_1^{x_1} b_2^{x_2} \equiv b_1^{x_1'} b_2^{x_2'} \bmod m_2 \ . \tag{28}$$

Since $b_1 \equiv 1 \bmod m_2$ by (20), (28) becomes

$$b_2^{x_2} \equiv b_2^{x_2'} \bmod m_2 \ .$$

However, the last congruence (20) shows that also b_2 is a primitive root $\bmod m_2$ and this shows that our last congruence contradicts our assumption (25) which completes the proof of our theorem.

Definition of the index I. The index of N is defined by the 2-dimensional vector

$$\text{ind } N = (x_1, x_2) \tag{29}$$

having $\varphi(m_1)\varphi(m_2) = \varphi(m)$ different values. Notice that x_i may be modified $\bmod \varphi(m_i)$ $(i = 1,2)$. We express this by saying that (x_1, x_2) is defined $(\bmod \varphi(m_1), \bmod \varphi(m_2))$. We also state the important

Corollary 1. 1. There is a one-to-one mapping of the $\varphi(m)$ elements

$$N \ \text{of a R.R.S.} \bmod m \ , \tag{30}$$

onto the set of $\varphi(m)$ indices

$$\text{ind } N = (x_1, x_2) \ , \tag{31}$$

where

$$x_i \ \text{runs through a R.R.S.} \bmod \varphi(m_i) \quad (i = 1,2) \ . \tag{32}$$

2. The set $\{N\}$ is a multiplicative group $\bmod m$, while the set of indices $\{(x_1, x_2)\}$ form an additive group $(\bmod \varphi(m_1), \bmod \varphi(m_2))$. The mapping

$$\{N\} \leftrightarrow \{(x_1, x_2)\} \tag{33}$$

is an isomorphism which transforms the multiplication $\bmod m$ in the first group into addition $(\bmod \varphi(m_1), \bmod \varphi(m_2))$ in the second group.

Remark. It should be clear how our discussion generalizes for a modulus

$$m = m_1 m_2 \cdots m_n \quad \text{with} \quad (m_i, m_j) = 1 \ \text{ if } \ i \neq j \tag{34}$$

and we assume that

(35) $\qquad a_i$ is a primitive root mod m_i $\quad (i = 1,\ldots,n)$,

while m certainly admits no primitive root if $n > 2$.

Thus for $n = 3$ the congruences (21) become

$$N \equiv b_1^{x_1} b_2^{x_2} b_3^{x_3} \bmod m, \quad (N \geq 1,\ N \leq m - 1)$$

$$\text{for } x_i = 0,1,\ldots,\varphi(m_i) - 1, \quad (i = (1,2,3) .$$

The corresponding Chinese Remainder problems (20) are

$$b_1 \equiv a_1 \bmod m_1, \quad b_2 \equiv 1 \bmod m_1, \quad b_3 \equiv 1 \bmod m_1 ,$$

$$b_1 \equiv 1 \bmod m_2, \quad b_2 \equiv a_2 \bmod m_2, \quad b_3 \equiv 1 \bmod m_2 ,$$

$$b_1 \equiv 1 \bmod m_3, \quad b_2 \equiv 1 \bmod m_3, \quad b_3 \equiv a_3 \bmod m_3 .$$

4. **Returning to the modulus 100.** By Lemma 1 we already know that the modulus 100 has no primitive roots. We wish to apply Theorem 1 to the numbers (8); that this is feasible is shown by (9) and (11). The congruences (20) become

$$
\begin{aligned}
b_1 &\equiv 3 \bmod 4, & b_2 &\equiv 1 \bmod 4\,, \\
b_1 &\equiv 1 \bmod 25, & b_2 &\equiv 2 \bmod 25\,,
\end{aligned} \tag{36}
$$

and are found to have the solutions

$$
b_1 = 51, \quad b_2 = 77\,, \tag{37}
$$

which are readily checked. Since $\varphi(4) = 2$ and $\varphi(25) = 20$, the main result (21), (22), of Theorem 1 shows that the congruences

$$
N \equiv 51^{x_1} 77^{x_2} \bmod 100, \quad x_1 = 0,1; \quad x_2 = 0,1,\ldots,19 \quad (1 \leq N \leq 99) \tag{38}
$$

furnish a R.R.S. mod 100.

The tables of indices I and numbers N are as follows.

Table of numbers N

(39)

$x_1 \backslash x_2$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	1	77	29	33	41	57	89	53	81	37	49	73	21	17	9	93	61	97	69	13
1	51	27	79	83	91	7	39	3	31	87	99	23	71	67	59	43	11	47	19	63

Table of indices (x_1,x_2)

(40)

N	1	3	7	9
0	0,0	1,7	1,5	0,14
1	1,16	0,19	0,13	1,18
2	0,12	1,11	1,1	0,2
3	1,8	0,3	0,9	1,6
4	0,4	1,15	1,17	0,10
5	1,0	0,7	0,5	1,14
6	0,16	1,19	1,13	0,18
7	1,12	0,11	0,1	1,2
8	0,8	1,3	1,9	0,6
9	1,4	0,15	0,17	1,10

The Table (39) gives the number N if $\text{ind } N = (x_1,x_2)$ is prescribed, where we locate x_1 in the first column and x_2 in the first row. The second Table (40) gives the index $I = (x_1,x_2)$ if N is given, where we locate the digit of tenth of N in the first column and its digit of units in the first row.

As an example let us find the product $N = 47 \cdot 27 \bmod 100$. Passing to indices we find $\text{ind } 47 = (1,17)$, $\text{ind } 27 = (1,1)$, and so $\text{ind }(47 \cdot 27) = (1,17) + (1,1) = (2,18) = (0,18)$. The first table gives the number $69 \equiv 47 \cdot 27 \bmod 100$.

As a more interesting application let us solve the congruence

(41) $$N^4 \equiv 61 \bmod 100 .$$

We pass to indices on both sides of the congruence setting $\text{ind } N = (x_1,x_2)$. From the second table we find $\text{ind } 61 = (0,16)$. We obtain

$$4(x_1,x_2) \equiv (0,16) \pmod{2, \bmod 20}$$

which gives the two congruences

$$4x_1 \equiv 0 \bmod 2, \qquad 4x_2 \equiv 16 \bmod 20 .$$

The first congruence has the two solutions $x_1 = 0, 1,$ and the second the four solutions $x_2 = 4, 9, 14, 19$. This gives the eight different indices $(x_1, x_2) = (0,4), (0,9), (0,14), (0,19), (1,4), (1,9), (1,14), (1,19)$. The table (39) gives the corresponding numbers and shows that (41) has the eight solutions $N = 41, 37, 9, 13, 91, 87, 59, 63$ hence

(42) $$N = 9, 13, 37, 41, 59, 63, 87, 91$$

which are readily checked on a hand-held calculator.

5. A circular slide-rule for the modulus 100. If the modulus m has a primitive root, then the mapping $\{N\} \leftrightarrow \text{ind } N$ is an isomorphism between the multiplicative group mod m, and the additive group mod $\varphi(m)$. The operation on the latter are nicely performed mechanically on a circular slide-rule. I can find no reference to this mechanical device, the only notable exception being B. M. Stewart's book [3] where the slide-rule nod 29 is described in Chapter 20. Notice the prime modulus $m = 29$ admits the primitive root $a = 2$.

For the modulus $m = m_1 m_2$, of (3), satisfying the assumption (5), the operations of the additive group of

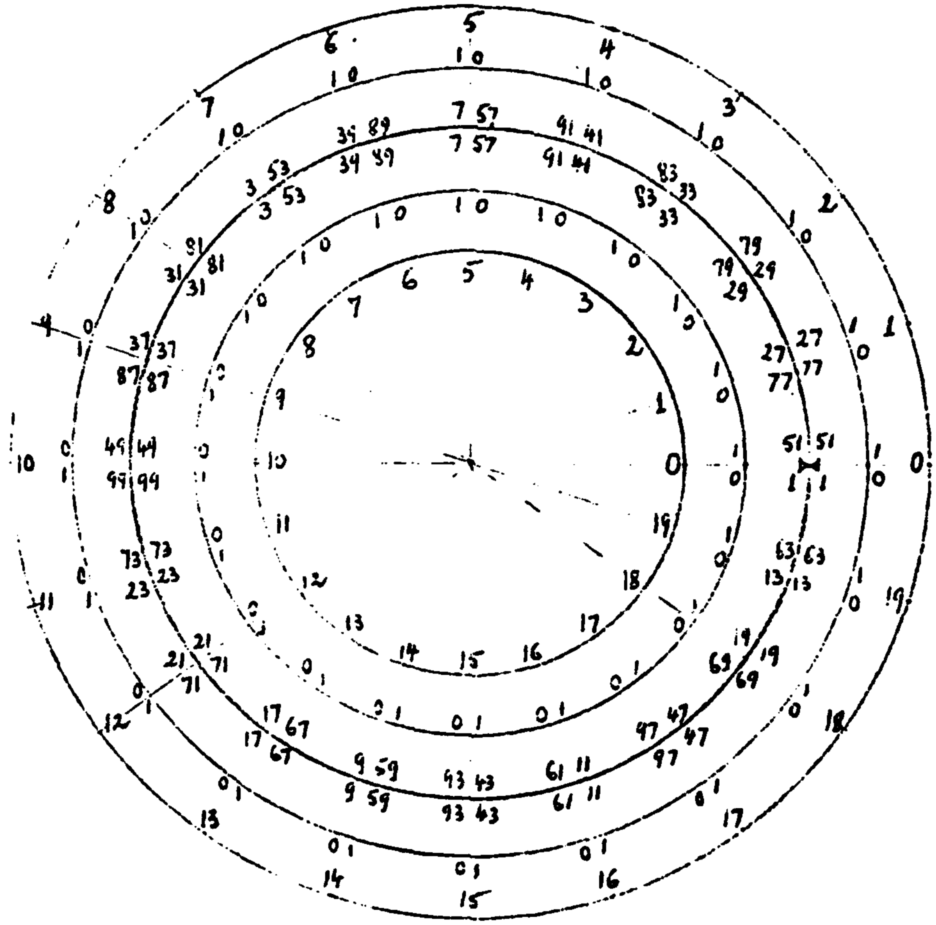
$$\text{ind } N = (x_1, x_2) \quad (\text{mod } \varphi(m_1), \text{ mod } \varphi(m_2))$$

can no longer be performed on a circular slide-rule. A notable exception is our modulus $m = 100 = 4 \cdot 25$ for the following reason: Here $\varphi(4) = 2$, and the operations on x_1 mod 2 can be done mentally, without mechanical aid.

The slide-rule mod 100 is shown in Fig. 1. It shows five increasing Concentric circle $C_1, \ldots, C_5$, each divided in 20 equal arcs. The slide rule must explicitly contain the $1 - 1$ correspondence between the set $\{N\}$ of $\varphi(100) = 40$ numbers and the set $\{I\} = \{(x_1, x_2)\}$ of 40 indices.

Along the points on C_1 and C_5 we place the 20 values of $x_2 = 0, 1, \ldots, 19$. Along every radius, like $x_2 = 3$ say, we place the corresponding values of x_1 and N, which are $x_1 = 0$, $N = 33$ and $x_1 = 1$, $N = 83$, respectively, which we find from table (39). The values 0, 33 are placed along C_4 and C_3, respectively, and we repeat them symmetrically with respect to C_3; likewise we place 1 and 83 near the radius of $x_2 = 3$, and repeat them by symmetry in C_3.

<u>Construction of the slide-rule</u>: We glue Fig. 1 on a piece of cardboard and cut the figure along the circle C_3 obtaining a disk D and a ring R. We glue the ring R onto a piece of cardboard and restore the disk D to its old place, with a pin in its center so that the disk can turn about its center. We also mark its initial position,



A circular Slide-Rule mod 100

Figure 1

for $x_2 = 0$, by two arrowheads. The slide-rule so obtained performs mechanically multiplications and division mod 100.

An example. To find

$$79 \times 37 \bmod 100$$

we locate 79 on C_3 and turn the disk by two divisions counter-clockwise until the initial arrowhead points to 79. The number 37 on the disk now points to the pair of possible products 73 and 23. Since for $N = 79$ we have $x_1 = 1$ and for 37 we have $x_1 = 0$, we conclude that for their product we have $x_1 = 1 + 0 = 1 \bmod 2$. This is why we select $N = 23$ rather than 73, and so

$$79 \times 37 = 23 \bmod 100 \ . \tag{43}$$

How did it work? The answer: From the slide-rule we see that for $N = 79$ we have $x_2 = 2$, and for $N = 37$ we have $x_2 = 9$; therefore for their product we have $x_2 = 2 + 9 = 11 \bmod 20$: On the slide-rule we performed the addition $2 + 9 = 11$. Thus for the product $x_2 = 11$ and this gave the possible products 73 or 23.

REFERENCES

1. Ulrich Oberst, Anwendungen des chinesischen Restsatzes, Expositiones Mathematicae 3 (1985), 97-148.

2. I. J. Schoenberg, The Chinese Remainder Problem and Polynomial Interpolation, to appear.

3. B. M. Stewart, Theory of Numbers, Second Edition, The Macmillan Co.. New York, 1964.

IJS:scr

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER 2955	2. GOVT ACCESSION NO. AD-A172771	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) ON THE THEORY AND PRACTICE OF MULTI-DIM. INDICES mod m. A CIRCULAR SLIDE-RULE FOR THE MODULUS m = 100		5. TYPE OF REPORT & PERIOD COVERED Summary Report - no specific reporting period
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) I. J. Schoenberg		8. CONTRACT OR GRANT NUMBER(s) DAAG29-80-C-0041
9. PERFORMING ORGANIZATION NAME AND ADDRESS Mathematics Research Center, University of Wisconsin 610 Walnut Street Madison, Wisconsin 53705		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS Work Unit Number 6 - Miscellaneous Topics
11. CONTROLLING OFFICE NAME AND ADDRESS U. S. Army Research Office P.O. Box 12211 Research Triangle Park, North Carolina 27709		12. REPORT DATE August 1986
		13. NUMBER OF PAGES 13
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Indices mod m as vectors
A circular slide-rule mod 100

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The paper establishes the following theorem of elementary Number Theory:

Let

(1) $$m = m_1 m_2, \quad (m_1, m_2) = 1$$

and let

(2) a_i be a primitive root mod m_i $(i = 1,2)$.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

20. **ABSTRACT** - cont'd.

We also assume that

(3) the modulus $m = m_1 m_2$ admits no primitive root .

By the Chinese Remainder Theorem applied twice we determine the solutions b_1 and b_2 of the two pairs of congruences

$$b_1 \equiv a_1 \bmod m_1, \quad b_2 \equiv 1 \bmod m_1 ,$$
$$b_1 \equiv 1 \bmod m_2, \quad b_2 \equiv a_2 \bmod m_2 .$$

Then every element N of a reduced residue system mod m is furnished just once by the congruences

(4) $$N \equiv b_1^{x_1} b_2^{x_2} \bmod m \quad (N \geqq 1,\ N \leqq m - 1) ,$$

where

(5) $$x_1 = 0,1,\ldots,\varphi(m_1) - 1, \quad x_2 = 0,1,\ldots,\varphi(m_2) - 1 ,$$

where $\varphi(m)$ is the Euler function.

We define the index of $N \bmod m$ as the 2-dim. vector

(6) $$\operatorname{ind} N = (x_1, x_2) .$$

Since b_i is a primitive root mod m_i $(i = 1,2)$ we can modify $x_i \bmod \varphi(m_i)$ $(i = 1,2)$.

The 1 - 1 mapping $\{N\} \leftrightarrow \{(x_1,x_2)\}$, established by (4), between the <u>multiplicative</u> group $\{N\}$ mod m and the <u>additive</u> group $\{(x_1,x_2)\}$ (mod $\varphi(m_1)$, mod $\varphi(m_2)$) is an isomorphism.

Using this theorem the paper concludes with the construction of a circular slide-rule for the modulus $m = 100$, which admits no primitive root.

END

11-86

DTIC